UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

FREE SPEECH COALITION, INC, et. al., *Plaintiffs*,	§	
v.	§	Civil Action No. 1:23-cv-00917-DAE
ANGELA COLMENERO, in her official capacity as Interim Attorney General for the State of Texas, *Defendant*.	§	

DECLARATION OF TONY ALLEN

1. I am over the age of 18 and have personal knowledge of the facts set forth in this Declaration.

2. I am a Chartered Trading Standards Practitioner and Global Subject Matter Expert on Age Assurance Systems. I am the Technical Editor of ISO/IEC 27566 — Information security, cybersecurity and privacy protection — Age assurance systems — Framework. I am the author of the Law of Age Restricted Sales in England and Wales.

3. I am also the Founder and Executive Director of the Age Check Certification Scheme, the leading UK Accreditation Service approved auditor and technology testing service for the global age assurance industry. I am also an audit member of the Age Verification Providers Association (AVPA) – the global trade association representing the age assurance industry.

4. I have personal knowledge of the history, process, and logistics of online age assurance (as defined herein).

EXHIBIT 4

5. I have also been closely involved in the development of age assurance legislation in the United Kingdom and elsewhere in the world, including the United States of America.

6. I have reviewed H.B. 1811, the Complaint, and Plaintiffs' Motion for Preliminary Injunction with its supporting declarations.

7. Based on my knowledge and experience, modern technology is capable of allowing providers of content, goods and services on the internet to verify the ages of their consumers without jeopardizing either the providers or consumers' interests in both free speech and privacy.

8. Further, the burden upon both providers of internet content, goods or services and consumers in verifying age is minimal, and reducing as technology evolves ever more.

9. Based on my knowledge and experience, software filters on devices, when properly installed, can be a useful parental tool in protecting children from online pornography, but in practice only provide a partial solution. They are less effective than, and not a substitute for, website-based age assurance which delivers a substantively different policy intent.

The availability of age verification services and how they work

10. Age Verification in the context of H.B. 1811 and defined more fully herein is the process by which the provider of internet content that is harmful to minors ("Content Provider") verifies that the consumer of the content is age 18 or older.

11. Age verification is not a new or rare technology. It is widely used by thousands of sellers and their consumers on a daily basis around the world, in a variety of contexts, such as alcohol and tobacco sales, gambling, gaming and, to a growing extent around the world, accessing pornography. I am aware that age verification is already actively deployed by many adult content service providers including Dorcel, Only Fans, Jacqui & Michel, StripChat, PornHub, MyDirty Hobby, Clips4Sale, MYM, Skokka, Live Jasmin, FanCentro, Loyal Fans, Viva Street and

xHamster, who are all subscribers to at least one Age Verification Provider, a company mentioned by the Plaintiff's called, Yoti[1]. These companies have applied age verification to one extent or another to their services elsewhere in the US, but also in the UK, France, Germany, Italy and in some cases, globally. PornHub have issued public information about their existing approaches to age verification[2].

12. Further, age verification providers continue to grow in number and continuously improve age verification technology. The Age Verification Providers Association began in 2018 with just six members. It now has twenty-four members and there are at least forty providers competing in the global market.

13. Age verification began in rudimentary style, perhaps with a faxed copy of a driver's license, but is now far more sophisticated, far less expensive, and employs robust safeguards for privacy concerns.

14. With the explosion of pornography on the internet, representative governments, including multiple states in the United States and many countries around the world, have looked for ways to protect children from harmful places on the internet, while simultaneously protecting rights of speech and privacy. The goal is to create safer places online where children can enjoy and benefit from the opportunities created by the worldwide web[3].

Privacy and the security of data

15. At the same time, Europe was implementing the General Data Protection Regulations ("GDPR"), a strict data protection regime requiring application of the principles of privacy-by-

[1] https://www.yoti.com/
[2] https://www.pornhub.com/press/show?id=2172
[3] https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5df252f14&appId=PPGMS

design and data minimization. This reinforced the need to devise a way to prove a user's age without disclosing their identity. In the United States, Consumer Privacy Protection Laws containing similar provisions, such as the CCPA (or California Consumer Privacy Act) are also now in place. In Texas, the Texas Data Privacy and Security Act (TDPSA) contains objectives to limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purpose of processing as disclosed to the consumer[4]. Consistent with these objectives, H.B. 1811 includes a requirement not to store personal data used for the purpose of age verification. See Texas H.B. 1811 § 29B.002(b)[5].

16. In light of the foregoing, the most straightforward solution was to create trusted Third-Party Servicers who would carry out the age checks, and then pass on only the outcome of those checks to the sites a user wished to visit. The various data protection laws globally, including in Texas, insist that providers only collect, process, and retain the data required for the specified purpose. So, generally where an Age Verification Provider obtained a consumer's personal information in order to confirm a user's age, it then had no further need to retain that data, and could delete it forthwith, storing only a user's account name, their age, and some form of password. This approach, therefore, does not require that all visitors to an adult website transmit to it their personal information and pre-empt any data breach similar to the example of Ashley Madison. [6]

17. Age Assurance Providers who are members of the AVPA and, thus sign up to its code of conduct[7], do not create new central databases when conducting age checks for the adult industry.

---

[4] See, Tex. H.B. 4, 88th Leg., 1st C.S. (2023)

[5] "(b) A commercial entity that performs the age verification required by Subsection (a) or a third party that performs the age verification required by Subsection (a) may not retain any identifying information of the individual" TEXAS H.B. 1811 § 29B.002(B).

[6] See, e.g., Kim Zetter, Hackers Finally Post Stolen Ashley Madison Data, Wired, Aug. 18, 2015, https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data

[7] https://avpassociation.com/membership/avpa-code-of-conduct/

There are, of course, sectors such as online gambling where regulators require audit trails, but H.B. 1811 requires, and indeed the industry's general practice is, not to retain any personal information after an age check is completed. These audited providers do not create new databases of personal data, nor track the behavior of individuals online.

18. During age verification processes, Age Verification providers apply the same degree of security you would expect in financial transactions.

19. Specifically, age verification companies must act to protect personal data and demonstrate their adherence to this through various forms of certification (e.g., ISO 27001, SOC2, CyberEssentials, BSI PAS 1296, etc.) to ensure personal data is dealt with securely.

20. In addition to local laws, such as GDPR in the UK and EU, there is an industry-wide certification protocol, operated by government approved auditors, which tests providers against international standards. This not only assesses the efficacy of the age check, but also of the data security and privacy measures. New standards are being developed by the IEEE and ISO which will ensure that age verification processes and procedures are kept up to date. Adult websites serving users in Texas may choose to use commercially available Age Verification providers certified by these regulatory bodies, not only to consolidate their defense against potential legal claims, but also to build consumer trust and confidence.

21. In 2017, the UK government passed the Digital Economy Act which included a provision that sought to ensure that minors could not normally access pornography without age verification. Both consumers and the adult websites themselves expressed concerns about privacy – particularly the risk that a treasure trove database of users' identities connected to the adult websites they chose to visit would be exposed by hackers. So, from the outset, privacy was a primary objective for those designing technical solutions for the age verification. Indeed, the Ashley Madison leak in

2015, cited by the Plaintiffs, was front of mind for the adult industry after seeing the user base of that site decimated by news of the breach.

22. Any question about whether an adult site is compliant with an age restricting law requires only a simple and straightforward audit of the verification process; no individual records or personal identifying information are needed.

23. Although Content Providers may perform Age Verification themselves, as set forth further below, Content Providers may, and often do, contract with third-party companies ("Age Verification Providers") to perform the service for a fee. These fees, discussed in paragraphs 56 to 63 of my declaration, are considerably lower than claimed in the Plaintiff's complaint. H.B. 1811 specifically allows for third-party verification. See (ibid) Texas H.B. 1811 § 29B.002(b).

24. When using an Age Verification Provider, a Content Provider directs the consumer to provide personal information directly to the Age Verification Provider who performs the verification and informs the Content Provider only of the result of the check – "pass" or "fail." It does not pass back the personal information. This is usually in response to a binary question (is this user over 18?) to which the answer can only be 'Yes' or 'No'. It is sometimes accompanied by a statement from the Age Verification Provider about how sure they are that their answer is correct (say 99% or 99.9%). It should be noted that whilst this statement can be a very high percentage, it will never be 100%.

25. The Age Verification Provider does not generally retain a consumer's personal Information other than the date of birth, which can be used to respond to subsequent enquiries about that user's age.

26. The verification process need only be performed once per user and, as discussed further herein, the verification results for any individual user may be shared among Content Providers and

other websites, thereby minimizing the need for multiple age verification checks of the same individual.

27. Users may be asked to authenticate when they wish to re-use a previously completed age check. This is the process of confirming the same user who completed the check is the current user. It can be achieved simply with a password or Personal Identification Number (PIN) or for a higher level of assurance, a biometric interaction such as how users currently open their cell phone.

Methods of available age verification

28. A number of methods have been developed, initially to verify age exactly, and more recently, to estimate it with an ever-increasing degree of accuracy.

29. Previous implementations of Age Verification solutions, such as in France where consumers are offered a range of methods from which to choose, showed consumers vary in their preferences of Age Verification method. A choice of methods, rather than a single one, led to greater adoption of age verification.

30. A choice of methods also addresses issues that arise from inclusivity, should any one method not be suitable for an individual.

Definitions of age verification

31. To assist the court with some terminology, I set out here the definitions and terms that are being included in international standards, including ISO/IEC 27566 – Age Assurance Systems – Framework (of which I am the Technical Editor). It is helpful to distinguish three related phrases:

a. "Age Assurance" is the process of establishing, determining, and/or confirming either age or an age range of a natural person.

b. There are three categories of Age Assurance:

i. "Age Estimation" is age determination performed using inherent features

or behaviors related to a natural person (where age determination is an indication that a natural person is over or under a certain age or within an age range).

ii. "Age Verification" is age determination based on the validity of a credential that provides information that allows the criterion to be tested.

iii. "Age Inference" is age determination based on the possession of something or access to something from which it can be inferred that only a person over 18 could have that.

32. Age Verification may be achieved by reference to drivers' licenses, passports, electoral rolls, credit reports, cell phone network records, banking, and credit card records. Users may also choose to create a digital identity, and selectively release just their age attributes.

33. Age Estimation, on the other hand, can be achieved by analyzing facial images, voiceprints or game play. The most advanced of these, facial estimation, is accurate to within +/-1 to 1.5 years mean absolute error, according to the latest published data by one certified age assurance provider, Yoti Limited. (https://www.yoti.com/wp-content/uploads/Yoti-Age-Estimation-White-Paper-March-2023.pdf). My certification team has independently verified and validated the results of this testing by Yoti.

34. The value of Age Estimation, as described more fully below, for both Content Providers and consumers is that it does not require consumers to submit any personal information other than suppling a live facial image or saying a short phrase to create a voiceprint.

35. There are a wide range of non-exclusive reasonable age verification methods that Content Providers and Third-Party Services can adopt to assure the ages of their users to varying degrees of certainty. These methods are used across the full range of situations where online age checks are required and have been certified by the Age Check Certification Scheme, which I manage.

36. Those which would be appropriate for implementing H.B. 1811 include the following;

a. Review of Government Issued Documents

A reliable, physical identity document can be reviewed, and the age details noted. Users will typically submit an image of one or more of these documents using a smartphone camera. Technology, known as optical character recognition (OCR) reads the data from the document which is then validated based on known security features built into the form of ID used. The photo on the document can also be compared to a freshly taken photo or video of the user, which is known as a "liveness" check. For the highest levels of assurance Near Field Communication (NFC) technology can be used to allow a smartphone to read a microchip in the document where this is available, and the data on the chip compared to the image on the document, and a fresh photo or video of the user.

b. Review of Credit reports and other private sector databases

In this method, users typically enter their name, address, and date of birth (Either specifically for the purposes of age verification or as part of their account opening or purchase process for the website they wish to access), and a search is made of credit reports or other reliable databases to confirm the details are accurate and obtain or confirm the date of birth. Often, this form of check is used where the user will need to be located at the address claimed as part of this process, to prevent users entering the information of other people, so it is well suited to the delivery of age-restricted goods.

c. Review of digital identity apps

Digital identity apps or wallets are being certified in certain parts of the world, e.g., UK, Europe, Australia, Singapore - these approaches can enable citizens to share their over or underage status; via selective disclosure, in a data minimized way. Based on information and belief, I understand that Texas does not yet have a state issued digital identification card or app.

d. Submission of Credit Card number

In many countries, credit cards are only issued to adults, so the possession and the ability to use a credit card is a potential indicator that someone is over 18, but it is worth noting that this is not universal.

e. Review of bank records

Banks generally require a strong level of identification check to open an account, and keep a record of their customers' dates of birth. Some banks allow trusted third parties to confirm a date of birth supplied to them by the customer with those records. Typically, the user logs into their own online banking system, and gives approval for the data to be supplied to the third party, which in this case would be the Age Verification Provider.

f. Age estimation via facial, voice, or behavioral analysis

It is important to be clear from the outset that age *estimation* technology is not a *recognition* technology; it detects and assesses information, to give an age estimation. This is expanded on below with a particular focus on facial age estimation.

A number of features and characteristics of people change with age. This allows for them to be analyzed to estimate age. An example of this is facial features. When facial age estimation is applied, users are either prompted to share a still or video image, or an existing profile picture can be used, and software then estimates their age. Systems learn how to do this by reviewing thousands of images of people with a known age to spot patterns common to those of the same age, and this means the technology is becoming better by the day. A live face is detected using liveness detection (as certified by International Standards) and then a pixel level review of the face is undertaken. The image generated by this method does not uniquely recognize any individual, so

is not deemed to be sensitive personal information by law and regulation, but in any event can and should be instantly deleted. In addition, this form of technology is not trained with associated names or addresses.

As stated above, facial age estimation is often falsely conflated with facial recognition technologies. In fact, the facial estimation technique described here is quite distinct from facial recognition. No image matching takes place for the purpose of estimating age.

Facial recognition may separately be used to check that a user relying on a previous age check is still the same individual who completed the check, but that is a separate process required for "authentication" rather than age estimation. Other estimation methods use voiceprints or analysis of how a user plays a computer game.

Presently, to meet a specific legal requirement for a person to be prevented from accessing material or services on the internet under a given age, increased confidence in the certainty of the age of a user of a site is possible by using systems that can be set with a "buffer" of an age level over and above the legally set age requirement. This approach will return a negative result if someone is estimated to be below the buffer age rather than below the legal threshold. The size of this buffer depends on the level of accuracy required by the Web service, or any regulatory requirements.

This method is inclusive of people of all ages, who do not own or have access to a government issued document. Age Estimation by facial or voice technology is one tool in a toolbelt. For example, for a law that requires a user to be aged 18 or older, such technology may be useful for

assuring that individuals are, say, 21 years or older even if the Content Provider and Age Verification Provider does not know their exact age. For those individuals, no further inquiry is needed. For those, however, whose facial or voice estimation results indicate an age range of under 21, then another Age Assurance method described herein may be used to confirm the exact age of the user.

37. Other methods of reasonable age verification, but which have not been subject to independent testing and certification, may include physical checks and vouching.

a. Physical Check

This is where a user is enrolled into an age assurance program in person. They may be asked to produce a physical proof of age which is checked by a trained member of staff, or it could be left to the judgement of staff to decide if someone looks at least 35, for example, who then certifies the user to be over 21.

b. Vouching

This is where other people with credibility are able to confirm a user's age. They may be professionals, such as teachers or doctors. It is one of the most inclusive methods of age verification, as users do not need to have any documents or particular records.

You can only vouch for someone if all of the following statements apply:

1. you have an existing relationship with the user;
2. you are sure the user is who they say they are;
3. you are in a position of authority in their community; and
4. you have proved your own identity

38. H.B. 1811 allows for a wide range of the reasonable methods described above, giving users a choice that suits their own circumstances and preferences, and ensures accessibility by not narrowly defining acceptable methods which could then exclude certain groups e.g., those without government-issued ID documents.

39. There are other methods of age assurance that are less reliable than those previously discussed and, subject to the facts of any specific subsequent case, may not amount to reasonable age verification methods for the purpose of H.B. 1811.

40. An example is known as Attestation or Self-Declaration. This is not considered a method that provides any assurance about the user's age, but can provide a starting point for the process, and in some cases where there is no risk in believing the answer given is accurate, it may still be fit-for-purpose. For example, if a child declares they are a child, then it may not be a problem to assume they are and protect them from harmful material on the internet. There are, however, sometimes good reasons to ensure children accessing websites on the internet are really children; for example, to prevent adults impersonating children online, so a more rigorous method is required.

41. Self-declaration is simply asking users to check a box, or enter their age or date of birth – without any additional checking against other data sources. Technical measures can improve reliability slightly – for example, allowing any year of birth to be entered, not only the year from before which the user would meet the site's minimum age requirement, or preventing users applying trial and error by repeatedly amending their age until they are admitted.

42. These weak methods of age assurance would not, on their own, achieve the level of accuracy required for robust age verification, which satisfies the principal international standard for age checks. They can be used in combination with other age assurance techniques, which is

why they are included in this summary, but on their own, they fall outside the scope of age assurance and the international standards the industry has developed.

Accuracy of methods, geolocation and circumvention

43. Each of these age verification methods, alone or in combination, verify age to a different level of certainty.

44. Regulators, or a regulated business, can determine this "level of assurance." For example, regulators or regulated businesses might use different processes for alcohol sales, gambling, pornography access, and knife, gun or ammunitions purchases.

45. The plaintiffs express a concern that "minors can use virtual private networks (VPNs), proxy servers, the "Tor" browser, and numerous other circumventions to bypass the Act's verification requirements with ease." Many online services already block traffic from well-known VPNs. For example, UK television channels the BBC and ITV[8] actively prevent users from pretending to be in a different geographical location in order to access content they would otherwise be unable to view from their real location. The most common way to achieve this is to look out for a single internet protocol (IP) address which is generating significantly more traffic than other IP addresses, which is a characteristic of most VPN traffic. There are specialist services that allow businesses to check if a user's IP address is associated with a VPN or TOR[9], as well as open-source lists[10] to assist sites which wish to prevent the use of VPNs. Generally, only more expensive, premium VPN services offer each user a new and unique IP address which is harder to

[8] "Potentially blocked up to 1M pirate viewers in the historic England v. Denmark Euro 2020 match" https://www.geocomply.com/resources/case-study/itv-tackles-streaming-piracy-with-geoguard/

[9] https://focsec.com/

[10] https://github.com/X4BNet/lists_vpn/blob/main/ipv4.txt

identify and block. These are considerably more expensive than the most widely used VPNs, making it harder for most minors to take advantage of their services.

46. The online gaming industry already makes extensive use of compliance services which require gaming operators to validate a customer's location to prove that the customer is located in a state or jurisdiction which permits online betting and gaming. One of the leading geolocation compliance providers is GeoComply. The company is licensed by state gaming regulators and its technology is tested for accuracy and adherence to regulatory standards. GeoComply conducts up to 1 billion geolocation transactions monthly from apps installed on 400m devices worldwide which allow a user to prove where they really are located. The company "Collects geolocation signals from multiple sources, including: GPS, WiFi, GSM, browser/HTML5 and IP address" to verify location accuracy. Further, GeoComply technology detects the use of location "spoofing" software or other methods of location obfuscation as is required under various state laws and regulations[11].

47. Age verification providers have invested heavily in anti-spoofing technology. This includes a number of techniques intended to reduce circumvention or 'spoofing' of age verification systems, including:

a. Liveness detection is generally deployed to ensure that where a facial image is used for facial age estimation, or is required for comparison with the photograph supplied as part of a government-issued ID, it is of a live human being who is presently using the device through which the age check is being completed.

[11] https://cdn.geocomply.com/wp/app/uploads/20230518141903/GeoComply-Core_Brochure_Gaming.pdf

b. Fake or altered documents are detected using a wide range of techniques. For example, AU10TIX employs a dual-layered defense against fake or altered documents. The aim is to combat not just visible fraud but also professional, organized-crime level of manipulations that employ advanced tools and possibly insider-expertise. AU10TIX case-level detection goes forensic in detecting altered as well as "manufactured" fakes, while AU10TIX traffic-level detection is detecting professional attack behavior, even when document manipulations are well hidden.

c. The combination of case-level forensics and traffic-level detection has shown that the currently known fraud statistics do not reflect the actual magnitude of fraud activity, with more sophisticated fraud (such as one utilizing generative AI Deepfake) technology actually showing constant increase "thanks" to the increasing availability of off-the-shelf tools.

d. Stolen documents can be detected by checking against published lists of compromised identity documents.

48. In general, the objective of most legislation in this field has been to ensure that sexually explicit content is not normally accessible by minors. In other words, most children should be prevented from seeing most adult content most of the time. Neither age verification nor age estimation techniques can guarantee 100 per cent accuracy, any more than staff in an adult bookstore are infallible when they check the age of their customers. But the technology is more than capable of preventing an adult website from knowingly giving access to children, as is the standard required in H.B. 1811[12].

[12] "CIVIL PENALTY; INJUNCTION. (a) If the attorney general believes that an entity is knowingly violating or has knowingly violated this chapter..." TEXAS H.B. 1811 § Sec.129B.006.

Re-usability

49. Businesses can offer their users a wide-range of privacy-preserving methods to estimate their age to a level of assurance that is proportionate to the level of risk presented by a site. Once an age verification check has been completed for one site, it is technically possible to re-use the outcome of that same check across any other website through a network that enables interoperability across websites through cooperation between their age verification technology suppliers. Regulators, standards bodies, or the interoperability networks themselves may place limits on the duration for re-use.

50. This approach means the technology exists now to ensure that H.B. 1811 does not threaten the principle of navigating seamlessly between many websites operated by unrelated entities. In effect, it asks users to take a small step, equivalent in the real world to wearing a seatbelt and using car seats, to protect children from online harm.

51. Historically, the Age Verification industry realized around 2020 that users may be willing to help a site assure their age if they wish to open an account that will last them a lifetime, but for sites they are just visiting temporarily, this could quickly become inconvenient and expensive. Recognizing this, the age verification industry has invested in delivering a mechanism that allows for the re-use of one age check across multiple websites.

52. A project was developed in six member states of the European Union, but has since opened up worldwide and includes major US companies to further develop the concept. The euCONSENT project, funded by the European Commission, was a successful proof of concept where 2,000 individuals from five countries visited three age-restricted websites in turn, relying on a check completed at the first site to access the other two. The project is now being put into live operation

in Europe, and a similar solution may be made available in the United States, as many states, including Texas, move to require age verification.

53. Users can choose to agree to accept a token on their device that merely indicates to websites they visit later that the user has already had their age verified, so these websites don't trouble the user again but instead ask the organization which did the first age check if this user meets their age condition. All this is done without sharing any identity details; nor is the user's age stored within the token to preserve their anonymity. As these are held locally on the device, there is no centralized 'honeypot' of data that could be the target of a hack (this is sometimes referred to as decentralized identity attributes). This significantly reduces the risk of data compromise at scale and, in any event, it only indicates that a user is over 18 and nothing about the reasons why they may have needed to prove that (it could be buying tobacco, gambling, gaming, car hire, accessing pornography or anything with an age-related eligibility criteria).

54. The age verification industry has developed reusable solutions and cooperated to develop and pilot interoperability so that age-assurance processes add little to no delay to a user's access to the internet, as their clients do not wish to drive any users away.

55. The convenience of interoperable and reusable age checks will avoid any problematic second-order effects. For example, this approach means that new websites and apps that users do not yet trust with their personal information need not ask them to provide it, as they will be able to rely on a check completed through a site that the user already trusts.

The Cost of Age Verification

56. The leading sector requiring robust age verification was online gambling. As an industry with a strong return per customer, it tolerated relatively high costs per age check, perhaps as much

as a dollar each. Naturally, as the Age Verification industry grew, competition put downward pressure on pricing, and it certainly halved relatively quickly.

57. Alongside competitive pressures, underlying costs were also falling. The earliest age verification methods almost all relied on accessing third party databases such as credit reports for which there was a substantial cost per check. The more successful providers secured volume discounts but were still facing a high fixed cost base. Naturally, providers looked for cheaper ways to deliver their services, so they looked beyond credit reports to banking and telecoms where good quality data was available at a much lower cost, or even at no variable cost at all.

58. The Plaintiff has set out a table of costs in their complaint (at paragraph 46). In my opinion, the Plaintiffs are quoting costs for identity verification here (sometimes referred to as 'Know-your-customer' (KYC) checks). These are of an order more expensive than age verification checks (which are merely verifying one attribute (your age) and not all aspects of your identity (like full legal name, address, previous addresses, marital status, credit, etc).

59. As a leader of an independent conformity assessment body, I cannot speak to the specific pricing offered by every individual provider, but the UK Government recently published an Impact Assessment for the Online Safety Bill which estimates the cost per check to be twelve cents (converted from pence), with a caveat this cost is expected to continue to fall through innovation, competition and interoperability. I am aware of some providers who offer age verification at no cost to certain sectors as part of a wider digital identity service and others have shared with me further details of their pricing which they are content to be shared in public.

60. Trustmatic, one of the providers quoted by the Plaintiff, have been willing to confirm that the plaintiff has incorrectly interpreted its pricing. Face biometric based age verification, according to their public pricing on our website, starts at EUR 0.39 per verification (for 100 monthly

verifications) and goes to EUR 0.14 per verification (for 30,000 monthly verifications). While this provider does not publicly publish pricing for volumes above 30,000 monthly, it has confirmed that it would charge EUR €18,000 for 100,000 verifications, not USD $40,000 as stated by the plaintiff. The claim that Trustmatic's pricing for 1M and 100M transactions is EUR 0.40 per TRX is therefore also incorrect. Their batch pricing for a batch of 1M transactions is EUR €50,000, or EUR 5 cents each; for a batch of 100M, they would charge €1 million, which is just 1 EUR cent each. To give a specific example, in order to help MindGeek fulfil legal obligations under the Bill, and to help address the issue of minors accessing restricted online content, Trustmatic would consider pricing of not more than EUR 3 cents per user to carry out selfie-based age checking on their users based in the State of Texas (subject to scoping – obviously this does not constitute a legally binding offer).

61. Yoti, another provider quoted by the Plaintiff, have confirmed to me that the pricing of £1.20 is quoted incorrectly, out of context and not relevant for this use case. The sterling £1.20 refers to list price i.e. for low volumes of document based identity verification checks (following the one-off upload of a government issued identity document and including identity document authenticity check, liveness detection, data extraction, face match). List pricing is where an organisation is not accessing any volume discounts - i.e. that would not be the case of a global adult site. Yoti state that their Age Verification Service (AVS) pricing ranges between $0.03 (for large volumes eg circa 100 M, $0.10 for circa 5M checks and $0.31 for lower volumes, one time account based checks e.g. under 100,000). They also offer free, $0.0 shares of 18 plus attributes from the reusable Yoti digital identity app, as explained below. The pricing will be dependent upon the age method, monthly volumes and whether the relying party is performing a one-time account based age check or an anonymized returning guest age check.

62. It is also important to highlight that adult content websites can be configured to recognize age attributes from certain age verification app wallets or data stores. These can sometimes be shared free of charge, including the Yoti app which is free for anyone sharing Over Age (eg Over 18). This is a one-time setup, taking 3-5 minutes, which can be created any time and thereafter reused to share age or identity details, privately, with relying parties across multiple industries.

63. The plaintiffs refer to a 700-word blog[13] by Jason Kelley, Activism Director at the Electronic Frontier Foundation, and its Senior Staff Attorney, Adam Schwartz, which argues that "there is no current method that does not carry inherent, unacceptable disadvantages and harms."

a. They claim that "This scheme [age verification] would lead us further towards an internet where our private data is collected and sold by default." This is unequivocally prevented by Age Verification providers not retaining centrally, in any new databases, personally identifiable information about the users, or any record of their online behavior. And where facial or voiceprint estimation methods are operated on a user's own device, personal data need not be shared even temporarily, and when it is, it is not retained by certified Age Verification providers.

b. The authors further state that "The tens of millions of Americans who do not have government-issued identification may lose access to much of the internet." which ignores the methods of facial and voiceprint age estimation and vouching, that can both enable undocumented people to verify their age online.

c. And they are concerned that "anonymous access to the web could cease to exist." The existing age verification industry has as its founding principle that the essence of age

[13] See, e.g., Jason Kelley and Adam Schwartz, Age Verification Mandates Would Undermine Anonymity Online, Electronic Frontier Foundation, March 10, 2023, https://www.eff.org/deeplinks/2023/03/age-verification-mandates-would-undermine-anonymityonline

verification is proving your age without disclosing your identity. The only information given to the sites a user wishes to access is "Pass" or "Fail" in answer to a question about their age qualification.

64. Furthermore, there is no "accessible ledger of adults who view adult content" created by the Age Verification industry, as the plaintiffs fear, because personally identifiable data is not retained. But even if the anonymized records of users who had proven their age online were somehow deciphered, it would offer only a list of adults who had variously purchased alcohol on the internet, placed a bet online, or any US parent or guardian of a child under the age of thirteen, to whom they had given consent to share their personal data under the Childrens Online Privacy Protection Act (COPPA)[14]. It would be a very long list and give no indication which subset of users had proven their age to access adult content.

65. While it is true that, as the complaint argues, "Hackers are targeting information shared on the internet at exponentially high rates," they are aware there is nothing of interest to be found by targeting certified Age Verification providers who store no personal data. The example given from Louisiana is of an attack on "MOVEIt" software which allows large amounts of data to be transferred, not of the LA Wallet.[15] Indeed, LA Wallet has confirmed to me that it was not affected by the recent MOVEit data breach[16].

[14] See 15 U.S.C. §§ 6501-6506 and 16 C.F.R. §§ 312.1-312.13

[15] "This attack, reportedly carried out by the Clop ransomware group, did not specifically target mobile driver's licenses in the state or anywhere else, but the nuances of data thievery, such as they are, might get lost on residents, many of whom are skeptical of things like mDLs [mobile Drivers Licenses]." https://www.biometricupdate.com/202306/theft-of-drivers-license-data-in-louisiana-could-be-a-big-test-for-digital-id

[16] https://nextsteps.la.gov/substitute-notice/

Adding the latest encryption techniques

66. In 2022, the French Data Protection Authority, published an article titled Online Age Verification: Balancing Privacy and the Protection of Minors, CNIL (Sept. 22, 2022), http://bit.ly/3EB1ISN [hereinafter CNIL Report].

67. The CNIL Report states:

a. "The CNIL also recommends, more generally, the use of a trusted independent third party to prevent the direct transmission of identifying data about the user to the site or application offering pornographic content. With its recommendations, the CNIL is pursuing the dual objective of preventing minors from viewing content that is inappropriate for their age, while minimizing the data collected on internet users by the publishers of pornographic sites."

b. "In order to preserve the trust between all of the stakeholders and a high level of data protection, the CNIL therefore recommends that sites subject to age verification requirements should not carry out age verification operations themselves but should rely on third-party solutions whose validity has been independently verified."

Age Verification around the world

68. The EU Better Internet for Kids Strategy mirrors the same desire as H.B. 1811: "Our vision is for age-appropriate digital services, with every child in Europe protected, empowered, and respected online, and no one left behind."

69. The UK Parliament expects to pass the Online Safety Bill in September 2023. This requires "highly effective" age verification or age estimation to prevent children from being exposed to "Primary Priority Content" on social media and adult sites. This content is initially to be defined as relating to suicide, self-harm, dieting and pornography. As when age verification was first developed at scale to prevent minors accessing adult websites, there remains a critical focus on

designing a solution that protects the privacy and data security of users, because this latest Bill is focused on children whose personal data is particularly sensitive. Maintaining the anonymity of children is a core design principle for the age verification sector.

70. It is also worth looking at countries such as Germany, where over 100 age assurance approaches have been reviewed and approved by the KJM regulatory body (https://www.kjm-online.de/aufsicht/technischer-jugendmedienschutz/unzulaessige-angebote/altersverifikationssysteme). There is clearly a healthy eco system of age assurance approaches and methods and many global companies, including some of those association members of the Plaintiff, which are already deploying age assurance approaches in many parts of the world.

71. There are many examples of increasing requirements for age verification for access to adult content online which are all aligned with Texas H.B. 1811.

Effectiveness of other methods

72. Other methods exist to advance the goal of protecting children from harmful material on the internet, including content filtering at the browser and/or the device level. These are parental controls. They can be device or browser based, applied to local routers in the home, or at the Internet Service Provider level. The last of these perhaps offers the ability to limit parental discretion by making decisions on what to filter that cannot be overturned by parents. This is already widely applied to block Child Sexual Abuse Material (CSAM) for example.

73. We know from repeated research by the UK's telecom's regulator, OFCOM, that many parents are unaware of this technology[17]. Those aware of it often do not know how to use it, or

[17] (https://www.ofcom.org.uk/__data/assets/pdf_file/0024/234609/childrens-media-use-and-attitudes-report-2022.pdf)

discover their children also know how to use it or have circumvented it some other way. And finally, those who know about it and know how to use it, must still choose to use it. "Just over a quarter of parents used content filters provided by their broadband supplier, where the filters apply to all devices using that service (27%). A much larger proportion (61%) said they were aware of this feature, showing that not all parents are adopting this potentially useful control." Children can be very persuasive, and parents might release the controls to allow them to play a game designed for 18+, unaware the game itself may be a portal to pornographic or other unsuitable content.

74. I do agree with the Plaintiffs that filtering technology includes not only Domain Name System (DNS) filtering, but also artificial intelligence (AI). However, it should be noted that DNS filtering fails when "DNS over HTTPS" is used to cloak a user's usage. This is easily adopted and has been standard for US users since 2019 if they use a Firefox/Mozilla browser, so this control is easily circumvented.[18]

75. The ability of AI, particularly if it only operates locally on the device, browser or router, to detect adult content is also limited. The most widely used approach is digital fingerprinting of known illegal content, for example using PhotoDNA, but this is limited to detecting known CSAM, Terrorist and other illegal content so cannot be considered to be AI based.

76. Filtering has proven an ineffective mechanism, as the level of exposure to adult content by minors clearly demonstrates. A survey of US parents by Kapersky in 2021 found that 48% used parental controls.[19] However, research from the Oxford Internet Institute, University of Oxford

[18] https://support.mozilla.org/en-US/kb/firefox-dns-over-https

[19] (https://usa.kaspersky.com/about/press-releases/2021_study-finds-50-of-parents-use-parental-control-apps)

has found that internet filtering tools are ineffective and in most cases, were an insignificant factor in whether young people had seen explicit sexual content[20].

77. Internet service providers are thus exploring many other methods for reducing the exposure of explicit material to general browsers. Google, as an example, has recently announced that it will blur by default search results containing sexually explicit content for all users, not only those who register as minors or turn on their "safe-search" facility[21].

What we've learned and what's changed in the last decade

78. The age-assurance methods discussed above do not necessarily add a new step to a user's visit to a new website or app because through re-usability and interoperability, one age check can be used across multiple sites seamlessly.

79. The user need only complete the age-assurance process once before they can reach their subsequent objectives. For websites and apps where users create accounts, the users may only have to complete the age-assurance process one time. After that, the website or app can store that the user is old enough to access it and authenticate the user when the user presents the login credentials associated with the account. Websites and apps that do not have user accounts need not force their users to repeat the age-assurance process each time the user tries to access the website or app because they can recognize when a user has previously completed an age check and rely on that check again.

80. The Act-mandated age-assurance need not require users to supply any private and sensitive information. For example, facial age estimation can be undertaken without any documentary

[20] Andrew K. Przybylski, Victoria Nash. Internet Filtering and Adolescent Exposure to Online Sexual Material. Cyberpsychology, Behavior, and Social Networking, 2018; 21 (7): 405 DOI: 10.1089/cyber.2017.0466

[21] https://techcrunch.com/2023/02/07/google-will-soon-blur-explicit-imagery-in-search-results-by-default/

evidence and either on a SAAS (software as a service) basis or entirely on a user's own device. The latter is offered by AVPA members, Privately and Yoti.[22] There is already technology in use to detect injection attacks (where a fake computer-generated image replaces that from a webcam) and prevent spoofing.

81. The state of Louisiana shows examples of premium and free platforms to view adult content sites deploying age assurance technology, to comply with state laws. In each instance where AVPA members are supplying the service, the adult operator receives an anonymized over age (18+) attribute to allow access to adult content.

82. Age verification technology is clearly working at scale globally, with both small and global brands, where it does not put user privacy at greater risk or merit the other criticisms levelled by the Plaintiffs. The decision to complete the age-assurance process can be an inherently risk-free one for users—i.e., users can select methods that do not require them to disclose personal and sensitive information.

83. Over the past 25 years, the age verification industry has developed a wider range of ways to verify age which offer users choice, including those who do not own or choose to use identity document-based approaches. They can choose, for example, age estimation techniques which do not require ownership or use of a document where the image is instantly deleted. Many hundreds of millions of age assurance checks are now undertaken globally each year. The cost has dropped dramatically, with reusability likely to lead to that trend continuing so there are no longer undue burdens on Web publishers due to the high costs of implementing age verification technologies. Nor would there necessarily be any significant loss of traffic resulting from the use of these

[22] *See* https://www.yoti.com/blog/safety-tech-challenge-fund-2021 and https://www.privately.eu/age-estimation/

technologies, except of course from children for whom the sites are unsuitable. The UK Government estimated in the Impact Assessment for legislation already approved by the House of Commons, a cost per check of twelve cents and lower for high volume platforms but noted cost may reduce further through interoperability and growing competition. The cost of that one 12 cent check may be defrayed across 100 websites before it might need to be repeated to maintain the ongoing integrity of the age verification ecosystem, and that is only if businesses determine that periodic re-validation is prudent.

84. Concerns about anonymity have also been addressed by developing age verification technology. The age verification sector was created specifically to enable users to access the sites they wished to access through the data minimized sharing of age. By selecting a trusted third party, even when selective disclosure from full identity document or digital identity wallet is used to prove age, the provider then only confirms "yes" or "no" when a website enquires "is this user an adult?" In Europe, users are given further reassurance by the enforcement of the General Data Protection Regulations (GDPR) but in the United States, contractual commitments to maintain secrecy and the threat of civil damages claims if that is not applied, offer similar protection.

85. And, of course, users may choose any of many other methods to prove their age, including facial age estimation where neither credit card numbers nor any personal data is required. Also, Age Verification standards allow for vouching where a user with no documentary proof of age can ask a respected member of their community such as a teacher or doctor to confirm their age.

86. H.B. 1811's age-assurance provision imposes some minimal implementation costs on regulated businesses with zero to minimal lag when a user first accesses an age restricted website – and perhaps, say annually, to revalidate their check.

Conclusion

87. H.B. 1811 does not radically change the internet's architecture, it merely makes it age-aware. It does not require users to share their full identity to go online and engage in constitutionally protected activities. Age checks online can, in fact, be completed in a more privacy-preserving manner than offline, because other personal data visible on a drivers' license is not shown in the process. Any privacy and security risks faced by both adults and children can be managed to the extent consumers demand – to the point with certain methods where there is no greater possibility of breaching either their privacy or security than already exists today when using the internet generally.

88. H.B. 1811 does not jeopardize First Amendment principles but applies the same principles for child protection we have in the real world to the growing online metaverse and should protect children from harm when taking advantage of the many benefits offered by the internet. Many of the Plaintiff's members are already embracing age verification technologies both elsewhere in the United States, but also globally.

DECLARATION UNDER PENALTY OF PERJURY

Pursuant to 28 U.S.C. §1746, I declare under penalty of perjury that the above statements are true and based upon my personal knowledge.

/s/_____
Tony Allen, Subject Matter Expert

Tony Allen
Tony Allen (Aug 18, 2023 15:32 GMT+1)
Aug 18, 2023

Texas - Adult - Declaration of Tony Allen FINAL

Final Audit Report 2023-08-18

Created:	2023-08-18
By:	Tony Allen (tony.allen@accscheme.org.uk)
Status:	Signed
Transaction ID:	CBJCHBCAABAA78Qo5Ehzt0cXggZRijZ_6aaemYRoxrLK

"Texas - Adult - Declaration of Tony Allen FINAL" History

Document created by Tony Allen (tony.allen@accscheme.org.uk)
2023-08-18 - 2:29:45 PM GMT- IP address: 150.220.172.34

Document emailed to tony.allen@accscheme.com for signature
2023-08-18 - 2:31:11 PM GMT

Email viewed by tony.allen@accscheme.com
2023-08-18 - 2:31:50 PM GMT- IP address: 150.220.172.34

Signer tony.allen@accscheme.com entered name at signing as Tony Allen
2023-08-18 - 2:32:09 PM GMT- IP address: 150.220.172.34

Document e-signed by Tony Allen (tony.allen@accscheme.com)
Signature Date: 2023-08-18 - 2:32:11 PM GMT - Time Source: server- IP address: 150.220.172.34

Agreement completed.
2023-08-18 - 2:32:11 PM GMT